Computing with Isogenies Between Abelian Varieties of GL$_2$-type

William Stein

July 11, 2011

Abstract

We lay the foundations for a computational theory of abelian varieties over $\mathbb{Q}$ of GL$_2$-type, or equivalently, with factors of modular Jacobians $J_1(N)$. This will make it possible to generalize Cremona’s tables of elliptic curves to higher dimension. We describe algorithms for enumerating and decomposing GL$_2$-type abelian varieties, isomorphism testing, computation of endomorphism and homomorphism rings, arithmetic with finite subgroups, computing the modular degree, computing special values of $L$-functions, and computing Tamagawa numbers. None of our algorithms use defining equations for varieties, and as such they work in a great degree of generality allowing us to treat all dimensions uniformly.

See http://wstein.org/talks/2004-02-04-CCR-ModAbVar/modabvar.pdf for a nice overview talk about what should eventually go in this paper.

1 Introduction

In this paper, we lay the foundations for a computational theory of abelian varieties over $\mathbb{Q}$ of GL$_2$-type. This will support generalizing Cremona’s highly influential tables [Cre97] of elliptic curves to higher dimension. We describe algorithms for enumerating and decomposing GL$_2$-type abelian varieties, isomorphism testing, computation of endomorphism and homomorphism rings, arithmetic with finite subgroups, computing the modular degree, computing special values of $L$-functions, and computing Tamagawa numbers. None of our algorithms use defining equations for varieties, and as such they work in a great degree of generality allowing us to treat all dimensions uniformly. There are also several open problems that are suggested by this paper [][give cross-references].

As mentioned above, a distinctive feature of our approach is that we do not use explicit defining equations. This is in stark contrast to the approach taken by many previous papers and theses [FpS+01] that treat only small dimensions. We also hope that some of the ideas in this paper may be applicable to [Edi00] and [?]. The methods in this paper are also used in the forthcoming paper [CS08]. The author has implemented all of the algorithms described here, and
they are included in Sage (which is free open source software [Ste07b]). [[Cite that whole French paper that does via ad hoc methods something like we do just for $J_0(125)$].]]

In this paper we mostly ignore issues of computational complexity, since our goal is to describe how it is practical at all to compute explicitly with modular abelian varieties. Except for [...? norm equations], the algorithm discussed in this paper mostly amount to linear algebra and have complexity that is polynomial time in the level $N$ of the abelian variety.

**Acknowledgement:** A very early draft of this paper was co-authored with Tseno Tselkov when he was an undergraduate at Harvard University. We thank Clement Pernet and Allan Steel for discussions about computation of Hermite and Smith normal form and saturation. Frank Calegari had many helpful ideas related to enumerating all abelian varieties in an isogeny class (see Section 3.1). We discussed solving norm equations with Claus Fieker.

### 1.1 GL$_2$-type and Modular Abelian Varieties

A simple abelian variety $A$ over $\mathbb{Q}$ is of GL$_2$-type if $\text{End}(A) \otimes \mathbb{Q}$ is a number field of degree equal to $\text{dim}(A)$. More generally an abelian variety is of GL$_2$-type if it is isogenous to a product of copies of simple abelian varieties of GL$_2$-type. Let $X_1(N)$ be the modular curve that parametrizes isomorphism classes of pairs $(E, P)$, where $E$ is an elliptic curve and $P$ is a point of order $N$, and let $J_1(N)$ be the Jacobian of $X_1(N)$, which is an abelian variety over $\mathbb{Q}$. An abelian variety $A$ over $\mathbb{Q}$ is modular if there is a homomorphism $A \to J_1(N)$ with finite kernel.

Ribet observed in [Rib92, §3] that every modular abelian variety is of GL$_2$-type. His paper also shows [Rib92 Thm. 4.4] that Serre’s conjectures [Ser87] on modularity of odd irreducible two-dimensional mod $p$ Galois representations imply the converse. Since Khare and Wintenberger have now completely proved Serre’s conjecture, we have the following theorem.

**Theorem 1.1** (Khare, Wintenberger). Every GL$_2$-type abelian variety over $\mathbb{Q}$ is modular.

Thus to explicitly compute with abelian varieties of GL$_2$-type it suffices to consider modular abelian varieties, which we do for the rest of this paper.

**Remark 1.2.** In this paper we only consider modular abelian varieties defined over $\mathbb{Q}$. It would be interesting to use similar methods to treat the general case of modular abelian varieties over a number field $K$, by which we mean abelian varieties $A$ over $K$ for which there exists a finite degree morphism $A \to J_1(N)$ over $K$ for some $N$. The main complication is that the endomorphism ring over $\overline{\mathbb{Q}}$ of a simple modular abelian variety $A$ over $\mathbb{Q}$ need not be commutative. Fortunately much is known about its structure (see [Rib80]).

Also many of the algorithms in this paper naturally generalize to the context of Grothendieck motives attached to modular forms. This is also a topic for future investigation.

2
1.2 Explicit Defining Data for Modular Abelian Varieties

We represent modular abelian varieties over $\mathbb{Q}$ explicitly as follows. Let $J$ be an arbitrary finite product of modular Jacobians $J_H(N) = \text{Jac}(X_H(N))$ for subgroups $H \subset (\mathbb{Z}/N\mathbb{Z})^*$, where $N$ is a positive integer (see, e.g., [1] for the definition of $J_H(N)$). We will refer to $J$ as an ambient modular abelian variety.

Fix a modular abelian variety $A$ and a finite degree homomorphism $\phi : A \to J$. Then there is an isogeny from the image $B$ of $A$ in $J$ back to $A$ whose kernel we denote by $G$, so $A$ is isomorphic to $B/G$ and $B \subset J$:

\[
\begin{array}{c}
J \\
\downarrow f \\
0 \rightarrow G \rightarrow B \rightarrow A \rightarrow 0
\end{array}
\]

In other words we can represent any modular abelian variety by giving $G \subset B \subset J$, all defined over $\mathbb{Q}$. It remains to explain how we explicitly specify $B$ and $G$.

We specify $B$ as follows. The inclusion $B \hookrightarrow J$ induces an inclusion of rational homology $H_1(B, \mathbb{Q}) \hookrightarrow H_1(J, \mathbb{Q})$ and $B$ is determined by the image $V$ of $H_1(B, \mathbb{Q})$ in the $\mathbb{Q}$-vector space $H_1(J, \mathbb{Q})$. We explicitly compute a basis for $H_1(J, \mathbb{Z})$ and $H_1(J, \mathbb{Q}) = H_1(J, \mathbb{Z}) \otimes \mathbb{Q}$ using modular symbols [St07a], and specify $B$ by giving a basis in reduced echelon form for a subspace $V \subset H_1(J, \mathbb{Q})$. Of course, not every subspace corresponds to a modular abelian variety, but we can determine whether or not a given $V$ corresponds to a valid abelian subvariety (see [??]).

We specify $G$ as follows. Suppose $V$ defines an abelian subvariety $B$ of $J$ as above. By the Abel-Jacobi theorem, we have

\[
J(\mathbb{C}) \cong H_1(J, \mathbb{R})/H_1(J, \mathbb{Z}),
\]

and letting $\Lambda = H_1(J, \mathbb{Z}) \cap V$ we have $B(\mathbb{C}) \cong (V \otimes \mathbb{R})/\Lambda$. In particular,

\[
B(\mathbb{C})_{\text{tor}} \cong V/\Lambda,
\]

and we specify $G \subset B(\mathbb{C})_{\text{tor}}$ by giving the lattice $L$ with $\Lambda \subset L \subset V$ such that $L/\Lambda \cong G$.

For brevity, henceforth we use the term modular abelian variety to mean a modular (or equivalently GL$_2$-type) abelian variety $A$ that has been given explicitly by a triple $(V, L, J)$ where $V \subset H_1(J, \mathbb{Q})$, the lattice $L \subset V$ contains $\Lambda = V \cap H_1(J, \mathbb{Z})$, and $J$ is specified by a finite ordered list of congruence subgroups $\Gamma_0(N)$, $\Gamma_1(N)$, and $\Gamma_H(N)$. We use the notation $(V, J)$ as a shorthand for $L = \Lambda$.

1.3 Contents

Turn this table of contents into prose when paper is done. (or maybe not.)
Contents

1 Introduction .................................................. 1
   1.1 GL2-type and Modular Abelian Varieties .............. 2
   1.2 Explicit Defining Data for Modular Abelian Varieties 3
   1.3 Contents ................................................ 3

2 Computing with Modular Abelian Varieties ............... 5
   2.1 Ambient Modular Abelian Varieties ..................... 5
   2.2 Enumerating New Simple Modular Abelian Varieties .... 6
   2.3 Decomposition .......................................... 6
      2.3.1 New and Old Subvarieties and Quotients ........ 6
      2.3.2 Decomposition as a Product of Simples .......... 6
      2.3.3 Verifying Defining Data of a Modular Abelian Variety 6
   2.4 Arithmetic with Modular Abelian Varieties ............ 6
      2.4.1 Sums and Products ................................ 6
      2.4.2 Intersection ....................................... 6
      2.4.3 Complements (Poincare Reducibility) ............ 7
      2.4.4 Quotients by Subgroups and Subvarieties ....... 7
   2.5 Finite Subgroups ....................................... 7
      2.5.1 Defining Data ..................................... 7
      2.5.2 The n-Torsion Subgroup .......................... 7
      2.5.3 Intersection of Finite Subgroups ................ 7
      2.5.4 The Cuspidal Subgroup ............................ 7
      2.5.5 The Rational Cuspidal Subgroup .................. 7
      2.5.6 The Torsion Subgroup ............................ 7
      2.5.7 The Shimura Subgroup ............................. 8
   2.6 Morphisms Between Modular Abelian Varieties ........ 8
      2.6.1 Defining Data for Morphisms .................... 8
      2.6.2 Natural Maps ...................................... 8
      2.6.3 Morphisms Defined by Finite Subgroups .......... 8
      2.6.4 Kernels of Morphisms ............................ 8
      2.6.5 Images of Morphisms ............................. 8
      2.6.6 The Universal Property of the Cokernel ......... 8
      2.6.7 The Projection Morphism ......................... 8
      2.6.8 Left and Right Inverses .......................... 8
   2.7 Endomorphism Rings and Hom Spaces .................... 8
      2.7.1 Computing End and Hom ............................. 8
      2.7.2 Computing Discriminants of Endomorphism Rings .. 11
      2.7.3 The Hecke Subring ............................... 11
      2.7.4 Atkin-Lehner Operators ........................... 11
      2.7.5 The I-torsion Subgroup for any Ideal I .......... 11
   2.8 Isogenies and Isomorphisms of Modular Abelian Varieties 11
      2.8.1 Isogenies From A to B ............................ 11
      2.8.2 Isomorphisms from A to B ....................... 12
      2.8.3 The Minimal Isogeny .................................. 14

4
2 Computing with Modular Abelian Varieties

2.1 Ambient Modular Abelian Varieties

modular symbols; \( \Gamma_H(N) \).
2.2 Enumerating New Simple Modular Abelian Varieties

Algorithm 2.1 (Enumerate Modular Abelian Varieties). Given a modular Jacobian $J$ this algorithm outputs a list of abelian subvarieties of $J$ in each isogeny class of simple modular abelian varieties of level $N$.

2.3 Decomposition

2.3.1 New and Old Subvarieties and Quotients

2.3.2 Decomposition as a Product of Simples

[[there is a very interesting algorithm here – this is related to verifying defining data]]

Algorithm 2.2 (Decompose as Product). Given a modular abelian variety $A$, this algorithm finds simple abelian varieties $B_i$ and an isogeny $A \to \prod B_i$.

2.3.3 Verifying Defining Data of a Modular Abelian Variety

2.4 Arithmetic with Modular Abelian Varieties

2.4.1 Sums and Products

[[problem – the input here should be $A = (V, L, J)$ and $A' = (V', L', J)$ in a common ambient $B = (V_2, L_2, J)$, where we need not assume $B \subset J$]]

Suppose $A = (V, J)$ and $A' = (V', J)$ are abelian subvarieties of a common ambient $J$. Then the $A + A' \subset J$ is given by $(V + V', J)$.

Suppose $A = (V, L, J)$ and $A' = (V', L', J')$ are modular abelian varieties. Then $A \times A' = (V \oplus V', L \oplus L', J \times J')$, where $V \oplus V'$ and $L \oplus L'$ embed diagonally into $J \times J'$.

2.4.2 Intersection

Suppose $A = (V, J)$ and $A' = (V', J)$ are abelian subvarieties of a common ambient $J$. Then $A \cap A'$ is an extension of the abelian variety $(A \cap A')^0 = (V \cap V', J)$ by a finite component group:

$$
\begin{array}{c}
0 \rightarrow (A \cap A')^0 \rightarrow A \cap A' \rightarrow \Phi \rightarrow 0,
\end{array}
$$

The component group is isomorphic to the torsion subgroup of kernel of the map $A \times A' \rightarrow J$ sending $(x, y) \rightarrow x - y$, which we compute using Section 2.6.4. In particular, we have

$$
\Phi \cong (\Lambda_J/(\Lambda_A + \Lambda_A'))_{\text{tor}}.
$$

[[this requires proof]] If $A$ and $A'$ are preserved by $\text{End}(J)$, then $\text{End}(J)$ also acts on $\Phi$ via its action on $\Lambda_J$. 

6
2.4.3 Complements (Poincare Reducibility)

[look in magma code to see how to do this. probably intersection pairing;]

2.4.4 Quotients by Subgroups and Subvarieties

Suppose $A = (V, L, J)$ is a modular abelian variety and $A' = (V', L', J)$ is an abelian subvariety of $A$, so $V \subset V'$ and $L' = L \cap V'$. Using Section 2.4.3 we compute $A/A'$ by finding a complement $B = (V_B, L_B, J)$ of $A'$ in $A$ along with surjective projection maps $\pi_{A'} : A \to A'$ and $\pi_B : A \to B$. Then the identity component of $A/A'$ is isomorphic to $B$. The component group $\Phi$ of $A/A'$ is isomorphic to the identity component of the kernel of the natural map $A \to B$, which we compute using Section 2.6.4.

2.5 Finite Subgroups

2.5.1 Defining Data
data: $(L \supset \Lambda, K, A)$.
morphisms between

2.5.2 The $n$-Torsion Subgroup

2.5.3 Intersection of Finite Subgroups

$G \cap H$

2.5.4 The Cuspidal Subgroup

2.5.5 The Rational Cuspidal Subgroup

i.e. $C(\mathbb{Q})$, which we can compute by getting $G_{\mathbb{Q}}$ action on $C(\overline{\mathbb{Q}})$.
arithmetic with: $G + H, G \cap H, G/H$.

2.5.6 The Torsion Subgroup

point counting over finite fields
divisor, multiple of order
2.5.7 The Shimura Subgroup

2.6 Morphisms Between Modular Abelian Varieties

2.6.1 Defining Data for Morphisms

2.6.2 Natural Maps

2.6.3 Morphisms Defined by Finite Subgroups

2.6.4 Kernels of Morphisms

2.6.5 Images of Morphisms

2.6.6 The Universal Property of the Cokernel

2.6.7 The Projection Morphism

2.6.8 Left and Right Inverses

2.7 Endomorphism Rings and Hom Spaces

2.7.1 Computing End and Hom

The following saturation algorithm will be important when computing \( \text{End}(A) \) and \( \text{Hom}(A, B) \).

[[insert very quick summary of Hermite and smith forms]]

[[this should go in paper on hnf, etc. writing with Clement Pernet]]

**Algorithm 2.3** (Saturate). Given a subgroup \( L \) of \( \mathbb{Z}^n \), this algorithm computes the saturation \((\mathbb{Q}L) \cap \mathbb{Z}^n \) of \( L \) in \( \mathbb{Z}^n \). Let \( M \) be a matrix whose rows are a \( \mathbb{Z} \)-basis for \( L \).

1. [Hermite Normal Form] Find the Hermite Normal Form \( H \) of \( M^t \).
2. [Inverse] Compute \( S = (H^t)^{-1}M \) using the “last big row” trick. Then output \( S \) whose rows are a basis for the saturation of \( L \).

**Proof.** It suffices to prove that \((H^t)^{-1}M \) has rows that span the saturation of the row span of \( M \). \[\square\]

Note that one could instead replace \( H \) by an LLL reduced basis for the rowspace of \( M^t \), but this is usually much slower because the \( p \)-adic/modular algorithm \[?] for computing Hermite normal form is fast.

If \( A \) is an abelian variety of dimension 2 then after choosing a basis for \( \Lambda = H_1(A, \mathbb{Z}) \), we have

\[
\text{End}(\Lambda) \cong \text{Mat}_{2d \times 2d}(\mathbb{Z}) \cong \mathbb{Z}^{(2d)^2}.
\]

**Proposition 2.4.** Let \( A \) be a simple abelian variety over a number field \( K \), let \( \Lambda = H_1(A, \mathbb{Z}) \) and embed \( \text{End}(A/K) \) in \( \text{End}(\Lambda) \) by the action of endomorphisms on homology. Then

\[
\text{End}(A/K) = (\text{End}(A/K) \otimes \mathbb{Q}) \cap \text{End}(\Lambda),
\]

where the intersection takes place in \( \text{End}(\Lambda) \otimes \mathbb{Q} \).
We will use the following lemma in the proof of Proposition 2.4.

**Lemma 2.5.** Let $K$ be a number field. If an element $x \in \mathbb{C}$ is fixed by every element of $\text{Aut}(\mathbb{C}/K)$, then $x \in K$.

**Proof.** If $x \in K$, this is standard Galois theory. If $x \notin K$, then $x$ is transcendental. Since $x + 1$ is also transcendental, the fields $\overline{K}(x)$ and $\overline{K}(x + 1)$ are isomorphic via a map $\sigma$ sending $x$ to $x + 1$. Every automorphism of a subfield of $\mathbb{C}$ extends to $\mathbb{C}$, so $\sigma$ extends to an automorphism of $\mathbb{C}$ that does not fix $x$. \qed

**Proof of Proposition 2.4.** An element of $\text{End}(A/\mathbb{C})$ is just a complex linear map on $\text{Tan}(A_{\mathbb{C}})$ that preserves $\Lambda$. The inclusion of $\text{End}(A/K) \otimes \mathbb{Q}$ in the right hand side is obvious, so suppose $\varphi \in \text{End}(A/K) \otimes \mathbb{Q}$ intersects $\text{End}(\Lambda)$. Then there is a positive integer $n$ such that $n\varphi \in \text{End}(A/K)$. Thus $n\varphi \in \text{End}(A/K) \otimes \mathbb{Q}$ induces a complex-linear endomorphism of $\text{Tan}(A_{\mathbb{C}})$, so $\varphi = (1/n)n\varphi$ also induces a complex-linear endomorphism of $\text{Tan}(A_{\mathbb{C}})$; also, by hypothesis $\varphi$ preserves $\Lambda$. Thus $\varphi \in \text{End}(A/\mathbb{C})$.

There is a nonzero integer $n$ such that $n\varphi$ is defined over $K$, so for any $\sigma \in \text{Gal}(\mathbb{C}/K)$, we have $\sigma([n]\varphi) - [n]\varphi = 0$. But
\[
\sigma([n]\varphi) = \sigma([n])\sigma(\varphi) = [n]\sigma(\varphi),
\]
so
\[
[n](\sigma(\varphi) - \varphi) = 0,
\]
which implies $\sigma(\varphi) = \varphi$, since the kernel of $[n]$ is finite and the image of $\sigma(\varphi) - \varphi$ is either infinite or $0$. By Lemma 2.5, $\varphi \in \text{End}(A/K)$. \qed

**Algorithm 2.6** (Endomorphism Algebra as Field). Given a simple modular abelian variety $A$ over $\mathbb{Q}$, this algorithm computes a number field $F$ and an isomorphism $\text{End}(A) \otimes \mathbb{Q} \to F$.

1. **[Find $A_f$]** Using Algorithm ??? find an isogeny $\varphi : A \to A_f$, where $A_f$ is a newform abelian variety.

2. **[Choose random endomorphism]** Randomly pick $[\text{[how??]}]$ an endomorphism $\varphi$ of $A_f$ and compute its minimal polynomial $g$.

3. **[Does endomorphism generate?]** If $\deg g = \dim(A_f)$, then let $F$ be the number field generated by a root $\alpha$ of $g$. Otherwise, go to step 1.

4. **[Define an isomorphism]** Let $\Psi$ be the unique field homomorphism $\text{End}(A_f) \otimes \mathbb{Q} \to F$ that sends $\varphi$ to $\alpha$. Compose this with the isomorphism $\text{End}(A) \otimes \mathbb{Q} \to \text{End}(A_f) \otimes \mathbb{Q}$ induced by $\varphi$ to obtain the desired isomorphism.

**Proof.** By [Rib92 ???] because $A$ is simple, modular, and defined over $\mathbb{Q}$, we know that $\text{End}(A) \otimes \mathbb{Q}$ is a number field of degree equal to $\dim(A)$. (If we instead consider $\text{End}(A/\mathbb{Q})$, then $\text{End}(A/\mathbb{Q}) \otimes \mathbb{Q}$ could be a non-commutative division algebra. Again we emphasize that by definition $\text{End}(A)$ contains only the endomorphisms of $A$ that are defined over $\mathbb{Q}$.)
By the primitive element theorem, there exists a $\varphi$ such that if $f$ is the minimal polynomial of $\varphi$, then $\deg(f) = \dim(A)$. Then since $\deg(f) = \dim(A)$ it follows that the map $\Psi$ is an isomorphism (a nonzero homomorphism between number fields of the same dimension is an isomorphism).

**Algorithm 2.7 (Compute $\text{End}(A)$).** Given a simple modular abelian variety $A$, this algorithm computes $\text{End}(A)$.

1. **[Find Modular Form]** Since $A$ is simple we can use Algorithm ?? to find a newform $f$ such that $A$ is isogenous to the abelian variety $A_f$. It suffices to compute $\text{End}(A) \otimes \mathbb{Q} = \text{End}(A_f) \otimes \mathbb{Q}$, since by Proposition 2.4 this yields $\text{End}(A)$. Thus it suffices to compute $\text{End}(A_f)$.

2. **[Initialize]** Let $d = \dim(A_f)$, let $n = 1$, and let $V$ be the zero subspace of $\text{End}(A_f) \otimes \mathbb{Q}$.

3. **[Compute Hecke operator]** Using Algorithm ??, compute the restriction of the Hecke operator $T_n$ to $A_f$, as an element of $\text{End}(A_f) \otimes \mathbb{Q}$.

4. **[Increase $V$]** Replace $V$ by $V + \mathbb{Q} \cdot T_n$.

5. **[Finished?]** If $\dim(V) < d$, increase $n$ and go to Step 3.

6. **[Saturate]** Compute $\text{End}(A_f/\mathbb{Q}) = V \cap \text{End}(A_f)$ using Algorithm ??.

**Proof.** We need to show that the algorithm terminates, i.e., that the Hecke algebra generates $\text{End}(A_f/\mathbb{Q}) \otimes \mathbb{Q}$. But by [Shi73, Thm. 1] the image of $T \otimes \mathbb{Q}$ in $\text{End}(A_f/\mathbb{Q}) \otimes \mathbb{Q}$ is a subfield of degree $\dim(A_f)$. But $A_f$ is simple by [Rib80, Cor. 4.2], so [Rib92, Thm. 2.1] implies that $\text{End}(A_f/\mathbb{Q}) \otimes \mathbb{Q}$ also has dimension $\dim(A_f)$. Thus the Hecke algebra generates $\text{End}(A_f/\mathbb{Q}) \otimes \mathbb{Q}$. By Proposition 2.4 once we have $\text{End}(A_f/\mathbb{Q}) \otimes \mathbb{Q}$ we apply Algorithm ?? to get $\text{End}(A_f/\mathbb{Q})$.

**Algorithm 2.8 (Compute $\text{Hom}(A, B)$).** Given modular abelian varieties $A$ and $B$, we compute $\text{Hom}(A, B)$ as follows.

1. **[Factorizations]** By Proposition 2.4 it suffices to explain how to compute $\text{Hom}(A, B) \otimes \mathbb{Q}$. For this, we compute using Algorithm ?? factorizations $\prod_{i \in I} C_i^{e_i}$ and $\prod_{i \in I} C_i^{f_i}$ of $A$ and $B$ up to isogeny (with isogenies) respectively, where $I$ is some index set, the $C_i$’s are non-isogenous simple abelian varieties, and $e_i, f_i \geq 0$. For the rest of this algorithm we replace $A, B$, by these products.

2. **[Simple case]** When $A \sim C^e$ and $B \sim D^f$, where $C, D$ are simple abelian varieties we compute $\text{Hom}(A, B)$ in the following way. If $C$ and $D$ are not isogenous $\text{Hom}(A, B) = 0$. If $C$ and $D$ are isogenous,

$$\text{Hom}(A, B) \otimes \mathbb{Q} = \text{Hom}(C^e, D^f) \otimes \mathbb{Q} = \text{Mat}_{e \times f}(\text{End}(C) \otimes \mathbb{Q}).$$
3. [General case] We compute each $\text{Hom}(C_{e_i}, C_{f_j}) \otimes \mathbb{Q}$ as in Step 2 and obtain $\text{Hom}\left( \prod C_{e_i}, \prod C_{f_j} \right) \otimes \mathbb{Q}$ as a matrix with blocks $\text{Hom}(C_{e_i}, C_{f_j}) \otimes \mathbb{Q}$ for each pair $(i, j)$.

Proof. Suppose first that $A \sim C^e$, $B \sim D^f$ with $C, D$ simple abelian varieties. When $C$ and $D$ are not isogenous there is no morphism $A \to B$, so $\text{Hom}(A, B) = 0$. When $C$ and $D$ are isogenous, a morphism $C^e \to D^f$ over $\mathbb{Q}$ is given by an $e \times f$ matrix with entries from $\text{End}(A) \otimes \mathbb{Q}$, where the $(i, j)$th entry represents the morphism between the $i$th component of $A$ and $j$th component of $B$. We get $\text{End}(A) \otimes \mathbb{Q}$ using Algorithm ??.

In general, when $A = \prod_{i \in I} C_{e_i}$ and $B = \prod_{i \in I} C_{f_i}$ we get $\text{Hom}(C_{e_i}, C_{f_j})$ as before and combining these blocks we obtain $\text{Hom}(A, B)$. 

### 2.7.2 Computing Discriminants of Endomorphism Rings

### 2.7.3 The Hecke Subring

computing its index; structure of quotient in full ring.

### 2.7.4 Atkin-Lehner Operators

### 2.7.5 The $l$-torsion Subgroup for any Ideal $I$

for $I \subset \mathcal{T}$ or $I \subset \text{End}(A)$.

### 2.8 Isogenies and Isomorphisms of Modular Abelian Varieties

#### 2.8.1 Isogenies From $A$ to $B$

**Algorithm 2.9** (Test if Isogenous). Given two modular abelian varieties $A$ and $B$, this algorithm decides whether or not $A$ and $B$ are isogenous, and if so returns an isogeny between them.

1. [A, B both simple] When $A$ and $B$ are both simple they are isogenous to abelian varieties $A_f$ and $A_g$ attached to newforms; we can find explicit isogenies using Algorithm ??$. Then $A$ is isogenous to $B$ if and only if $A_f = A_g$, i.e., $f$ and $g$ are Galois conjugate.

2. [Pair off factors] When $A$ and $B$ are not simple we pair off factors, i.e. for any $C$ in a factorization of $A$ we check if there is an isogenous $D$ in a factorization of $B$. If such $D$ exists and the multiplicities of $C$ in $A$ and $D$ in $B$ are the same we remove $D$ and continue with another $C$. Otherwise, $A$ and $B$ cannot be isogenous.

Proof. When $A$ and $B$ are simple, by [Fal86, §5] $A \simeq A_f$ and $B \simeq A_g$ are isogenous if and only if the corresponding newforms $f$ and $g$ are Galois conjugate, since $f$ and $g$ determine $L(A_f, s)$ and $L(A_g, s)$. 

11
If $A \sim \prod_{i \in I} A_i^{e_i}$ and $B \sim \prod_{i \in I} B_i^{e_i}$, indexed so that $A_i \sim B_i$ for all $i \in I$, then we get that the products $\prod_{i \in I} A_i^{e_i}$ and $\prod_{i \in I} B_i^{e_i}$ are isogenous, so $A$ and $B$ are also isogenous.

Conversely, suppose that $A \sim B$ and $\varphi : A \to B$ is some isogeny. Let $A \sim \prod_{i \in I} A_i^{e_i}$ and $B \sim \prod_{j \in J} B_j^{f_j}$ be factorizations of $A$ and $B$ into products of powers of non-isogenous simple abelian varieties. Fix an index $i \in I$. Combining the maps from $A_i$ to $A_i$, from $A$ to $B$, and the projection to $B_j$ for each $j$ we obtain morphisms $\phi_{ij} : A_i \to B_j$ for all $j \in J$. Since the image of an abelian variety is an abelian variety and all $B_j$’s are simple it follows that $\varphi_{ij}(A_i)$ is either zero or all of $B_j$, which means that $A_i$ and $B_j$ are isogenous. It is not possible that all $\varphi_{ij}(A_i)$ are zero since that would imply that $\varphi$ is the zero map, so we find a $B_j$ isogenous to $A_i$. Removing $A_i$ and $B_j$ from the factorizations and repeating this argument yields that $A$ and $B$ are isogenous if and only if there is a bijection $\sigma : I \to J$ such that $A_i$ is isogenous to $B_{\sigma(i)}$ for all $i$, and $e_i = f_{\sigma(i)}$.

### 2.8.2 Isomorphisms from $A$ to $B$

In this section we describe an algorithm to decide whether two simple modular abelian varieties are isomorphic, and if so to give an isomorphism. We do not yet know an algorithm to decide whether two nonsimple modular abelian varieties are isomorphic (just need a way to enumerate elements in lattice of small norm – might be straightforward if don’t care about speed!).

**Algorithm 2.10 (Norm Equation).** Given an order $\mathcal{O}$ in a number field $K$ and an element $a \in \mathbb{Q}$, this algorithm finds all solutions in $\mathcal{O}$ to the norm equation $\text{Norm}(x) = a$, up to units of $\mathcal{O}$.

Replace the following by a reference to Henri Cohen’s book, etc. [[Claus Fieker suggests the following algorithm (we should expand on that)]

1. [Class Group] Find the class group of $K$.
2. [Ideals of bounded norm] Use linear programming [[huh??]] to find all ideals of norm up to some bound.
3. [Solve] Deduce all solutions to the norm equation up to units.

**Algorithm 2.11 (Test if Isomorphic).** Given simple modular abelian varieties $A$ and $B$, this algorithm either proves that $A$ and $B$ are not isomorphic, or returns an isomorphism between them (or all isomorphisms, up to units).

1. [Equal?] If $A = B$, return “yes” and the identity map.
2. [Isogenous?] Determine whether $A$ and $B$ are isogenous using Algorithm ??.
   If $A$ and $B$ are not isogenous then return “no”, and if $A$ and $B$ are isogenous, let $f : B \to A$ be an isogeny.
3. [Degree of isogeny] Compute $d = \deg(f)$. If $d$ is not a square, return “no”.

4. [Endomorphism algebra] Compute the number field $K = \text{End}(A) \otimes \mathbb{Q}$, and an embedding of $\text{End}(A)$ into $K$ using Algorithm ??.

5. [Hom space] Compute $\text{Hom}(A, B)$ using Algorithm ??.

6. [Image of Hom space] Compute the image $H_f$ of $\text{Hom}(A, B)$ in $\text{End}(A)$ got by composing with $f$.

7. [Endomorphism ring] Compute the order $\mathcal{O}$ in $K$ equal to $\text{End}(A)$ using Algorithm ??.

8. [Solve norm equation] Find solutions (up to units of $\mathcal{O}$) of the norm equations $\text{Norm}(x) = \pm \sqrt{d}$ in $\mathcal{O}$. If there are no solutions, return “no”.

9. [Lift to $H_f$?] For each solution (up to units), check whether it lies in $H_f$.

10. [Isomorphic?] If a solution $x$ lies in $H_f$, then return “yes” and $x \circ f^{-1}$.
    (Note that at this point we could also output $x \circ f^{-1}$ and continue on to return representatives for all isomorphisms up to units.)

11. [Not isomorphic?] If none of the solutions lies in $H_f$, return “no”.

**Proof.** Let $f : B \to A$ be an isogeny and denote its degree by $d$. Define

$$H_f = \{ f \circ g : g \in \text{Hom}(A, B) \} \subset \text{End}(A).$$

Since degree is multiplicative, $A$ and $B$ are isomorphic if and only if the subset $H_f$ of $\text{End}(A)$ contains an element of degree $d$. Embed $\text{End}(A)$ into the number field $K = \text{End}(A) \otimes \mathbb{Q}$ and let $\mathcal{O}$ be the order in $K$ that is the image of $\text{End}(A)$. By [Mil86, Prop 12.12], for $x \in K$ we have $\text{Norm}(x)^2 = \deg(x)$. Thus, finding an element of degree $d$ in $H_f$ is equivalent to finding $x \in \mathcal{O}$ with $\text{Norm}(x) = \pm \sqrt{d}$, such that $x \in H_f$, where we view $H_f$ as a subset of $K$ using the above inclusions. Using Algorithm ??, we find all $x$ such that $\text{Norm}(x) = \pm \sqrt{d}$, up to units of $\mathcal{O}$. There are may be infinitely many units, e.g., if $K$ is a real quadratic field, so there are often infinitely many solutions to the norm equation and we cannot directly check whether at least one of these infinitely many are in $H_f$. However, because there are only finitely many solutions up to units, it will suffice to show that $H_f$ is stable under units and to check whether each representative solution is in $H_f$. Thus to finish the proof of correctness of the algorithm, we verify that $x \in H_f$ if and only if $xu \in H_f$, where $u$ is any unit of $\mathcal{O}$. If $x = f \circ g$ for some $g \in \text{Hom}(A, B)$, then $xu = f \circ (g \circ u)$ is in $H_f$ since $g \circ u \in \text{Hom}(A, B)$. Conversely, if $xu \in H_f$, then by what we have just shown $x = xuu^{-1} \in H_f$. 

Discuss how non-simple case works. Still just need to solve a norm equation but solving it is more complicated (?)
2.8.3 The Minimal Isogeny

A small extension of Algorithm ?? gives us the minimal degree of any isogeny between two isogenous modular abelian varieties. [[delete below and just say that we run through all square multiples of \(d\) instead of just \(d\) in the algorithm above. the below is riddled with errors anyways.]]

**Algorithm 2.12** (Minimal Isogeny). Given simple modular abelian varieties \(A\) and \(B\), this algorithm checks if \(A\) and \(B\) are isogenous and if so returns the minimal degree of an isogeny \(A \to B\) together with an isogeny of that degree.

1. [Equal?] If \(A = B\), return 1 and the identity map.
2. [Isogenous?] Determine whether \(A\) and \(B\) are isogenous using Algorithm ??.
   If \(A\) and \(B\) are not isogenous then return “not isogenous”, and if \(A\) and \(B\) are isogenous, let \(f : B \to A\) be some isogeny.
3. [Degree of some isogeny] Compute \(\deg(f)\) using Algorithm ??.
   Write \(\deg(f) = ab^2\), where \(a\) is squarefree.
4. [Endomorphism algebra] Compute the number field \(K = \text{End}(A) \otimes \mathbb{Q}\), and an embedding of \(\text{End}(A)\) into \(K\) using Algorithm ??.
5. [Hom space] Compute \(\text{Hom}(A, B)\) using Algorithm ??.
6. [Image of Hom space] Compute the image \(H_f\) of \(\text{Hom}(A, B)\) in \(\text{End}(A)\) got by composing with \(f\).
7. [Endomorphism ring] Compute the order \(O\) in \(K\) generated by \(\text{End}(A)\) Algorithm ??.
8. [Initialize] Let \(i = 0\).
9. [Solve norm equation] Increase \(i\) by one and find the solutions (up to units of \(O\)) of the norm equations \(\text{Norm}(x) = \pm abi\) in \(O\). If there are no solutions, repeat this step.
10. [Lift to \(H_f\)?] For each solution (up to units), check whether it lies in \(H_f\).
11. [Isogenous of degree \(a^2i^2\)] If a solution \(x\) lies in \(H_f\), then return \(a^2i^2\) and \(x \circ f^{-1}\).
12. [Should try isogeny of higher degree] If none of the solutions lies in \(H_f\), return to Step 9.

**Proof.** Let \(f : A \to B\) be an isogeny and denote its degree by \(d = ab^2\), where \(a\) is squarefree. Define \(H_f = \{ \phi \circ f : \phi \in \text{Hom}(B, A) \} \subset \text{End}(A)\). Since degree is multiplicative, \(B\) and \(A\) are isogenous via an isogeny of degree \(d\) if and only if \(H_f\) contains an element of degree \(dd'\). Embed \(\text{End}(A)\) into \(K = \text{End}(A) \otimes \mathbb{Q}\) and let \(O\) be the order in \(K\) generated by \(\text{End}(A)\). By Proposition 12.12. in Milne’s ”Abelian Varieties” for \(x \in K\) we have \(\text{Norm}^2(x) = \deg(x)\). Thus,
finding an element of degree \(d'd\) in \(H_f\) is equivalent to finding \(x \in \mathcal{O}\) with
\(\text{Norm}(x) = \pm \sqrt{d'd}\), such that \(x\) actually comes from \(H_f\). Hence, the possible
values for \(d'\) are \(ai^2\) for \(i \in \mathcal{N}\). We can find all \(x\) such that \(\text{Norm}(x) = \pm \sqrt{d'd}\)
up to units of \(\mathcal{O}\). The proof that this suffices is the same as the end of the proof
of Algorithm 2.11.

2.9 Complex Periods

2.9.1 The Period Lattice

Compute period lattice numerically

2.9.2 The BSD Real Volume

BSD real volume \(\Omega_A\) – possibly just use Dokchitser and \(L(A,1)/\Omega_A\) via modular
symbols. \([dokchitser\ no\ good\ –\ not\ rigorous.\]"

2.10 Component Groups

2.10.1 Supersingular Curves

2.10.2 Definite Quaternion Algebras

describe algorithm; will finally have to implement something in sage if I’m to
compute the tables at the end.

Basically this sec is just a quick reference to Pizer, Kohel, Dembelle.

2.10.3 The Component Group

cite my other papers on this topic and give some examples.

2.10.4 Tamagawa Numbers

2.10.5 \(J_1(N)\)

include stuff about \(J_1\) from conrad-edixhoven-stein. generic bounds. no real
theory?

Mention open problems.

2.11 Complex \(L\)-Series

2.11.1 Local \(L\)-factors

via characteristic poly of Frobenius in complete generality: factor as newform
abvars, use Hecke polys

2.11.2 Numerical Evaluation at any Point

anywhere (via Dokchitser)
2.11.3 The Rational Part of the Special Value
(generalize Agashe-Stein?)

2.11.4 Order of Vanishing (Analytic Rank)

2.11.5 Zeros in the Critical Strip
(Rubinstein)

2.12 \( p \)-adic \( L \)-Series

2.12.1 The Definition

2.12.2 Computing to Given Precision

Factor up to isogeny using newforms; compute series for that, except if there is a \( p \) in isogeny degree, in which case give up (?) or? Generalize wuthrich-stein to dimension > 1. Help from Robert Bradshaw.

[[Do the computation in \( M[T] \) where \( M \) is a modular symbols module, like in Mazur-Tate-Teitelbaum. It’s just that sum and projection.]]

2.12.3 Computing the Leading Coefficient and Order of Vanishing

3 Computing the Isogeny Class

Discuss problem of finding lots of non-isomorphic \( A \) in the isogeny class of \( A_f \).

Various ways to compute finite Gal(\( \overline{\mathbb{Q}} / \mathbb{Q} \))-stable subgroups of \( A \). (I.e., kernel of maps to higher level \( Np \). Intersection with other \( A_g \)'s. Intersection with (or image of) cuspidal subgroup, Shimura subgroup, cut out using Hecke operators when the dimension is bigger than 1, etc.)

Example 3.1. We show that the \( \mathbb{Q} \)-isogeny class of 43B contains at least three non-isomorphic abelian varieties.

[[replace by sage]]

> J := JZero(43);
> A := J(2);
> A;
Modular abelian variety 43B of dimension 2, level 43 and conductor 43^2 over \( \mathbb{Q} \)
> G := RationalCuspidalSubgroup(A);
> G;
Finitely generated subgroup of abelian variety with invariants [ 7 ]
> B := A/G;
> B;
Modular abelian variety of dimension 2 and level 43 over \( \mathbb{Q} \)
> IsIsomorphic(A,B);
false
> A_dual := Dual(A);
> IsIsomorphic(A_dual,A);
true Homomorphism from modular abelian variety of dimension 2 to 43B given on integral homology by:
[ 1  0 -2 -1]
[ 1  0 -3 -1]
[ 0  2 -2 -1]
[ 0  1 -1 -1]
> B_dual := Dual(B);

>> B_dual := Dual(B);

Run-time error in 'Dual': The modular embedding of argument 1 must be injective.
> J2 := JZero(43*2);
> phi := NaturalMap(J,J2,1);
> phi2 := NaturalMap(J,J2,2);
> H := Kernel(phi-phi2);
> H;
Finitely generated subgroup of abelian variety with invariants [ 7 ]
> A;  
Modular abelian variety 43B of dimension 2, level 43 and conductor 43^2 over Q
> A/H;
Modular abelian variety of dimension 2 and level 43 over Q
Homomorphism from 43B to modular abelian variety of dimension 2 given on integral homology by:
[ 1  0  1  0]
[ 1 -1  0 -1]
[ 1 -1 -1  1]
[ 1  1 -1  0]
Homomorphism from modular abelian variety of dimension 2 to 43B given on integral homology by:
[ 3  1  1  2]
[ 1 -2 -2  3]
[ 4 -1 -1 -2]
[ 2 -4  3 -1]
> C := A/H;
> IsIsomorphic(A,C);
false
> IsIsomorphic(B,C);
false
> G;
Finitely generated subgroup of abelian variety with invariants [7]
> H;
Finitely generated subgroup of abelian variety with invariants [7]
> G eq H;
false
> G +H;
Finitely generated subgroup of abelian variety with invariants [7, 7]

3.1 The Class Group – Noneisenstein Isogenies

Here we make this more precise. Suppose that $N$ is prime. Let $A$ be a simple modular abelian variety and let $f$ be the associated normalized newform. Denote by $O$ the finite $\mathbb{Z}$-algebra generated by the coefficients of $f$ and consider $H = \text{Cl}(O)$. Let $S = \{q_i\}$ be a set of representatives for $H$ such that $q_i$ has odd residual characteristic and is non-Eisenstein. Then the following proposition describes all possible simple abelian varieties that are isogenous to $A$ with an isogeny whose kernel has support outside the Eisenstein primes and primes of residual characteristic 2.

**Proposition 3.2.** Let $\varphi : A \to A'$ be an isogeny whose kernel has support outside the Eisenstein primes and primes of residual characteristic 2. Then $A' \simeq A/A[q]$ for some $q \in H$.

This method gives us at least part of the isogeny class. [[Note that at the end of his notes Frank mentions a relation between the Eisenstein primes and non-trivial isogenies.]]

3.2 Eisenstein Isogenies

Quotient out by any subgroup of the cuspidal subgroup.

Quotient out by any subgroup of the Shimura subgroup $\Sigma$. The Shimura subgroup is by definition the kernel of the natural map $J_0(N) \to J_1(N)$ induced by $X_1(N) \to X_0(N)$. Paper Ling and Oesterlé that describes $\Sigma$ in computable terms directly at level $N$.

Suppose $A, B \subset J_0(M)$ are simple and non-isogenous, for some $M$. Then $A/(A \cap B)$ is isogenous to $A$.

Remark: Kernels of endomorphisms have square degree. So quotienting out by any rational subgroup of nonsquare order gives a nontrivial isogeny. Get these from $C$. 

18
3.3 Enumerating the Isogeny Class

Do all the operations above suffice to enumerate all elements of any isogeny class? If not, what do we miss.

4 Tables of Modular Abelian Varieties

4.1 Contents

For each $N \leq 125$ (say), compute all modabvars for $J_0(N)$. Also for each $N \leq 49$ (say), compute all modabvars for $J_H(N)$ for all $H$. Also do $J_0(389)$, say. For each compute:

1. Field $F = \text{End}(A) \otimes \mathbb{Q}$; $\text{disc}(F)$; description of $O = \text{End}(A) \subset F$ and of $\mathbb{T}' \subset \text{End}(A)$.

2. first few coefficients of $q$-expansion

3. all non-isomorphic elements of the isogeny class (found using our methods), which we label

4. a graph showing the isogenies with their structure (degree, etc.)

5. the matrix showing structure of intersections between all simple new abvars of level $N$

6. index of $\mathbb{T}$ in $\text{End}(A_f)$

7. discriminant of $\text{End}(A_f)$

8. modular degree; modular kernel with Hecke action (?)

9. cuspidal subgroup

10. rational cuspidal subgroup

11. torsion subgroup (if possible)

12. real volume to some precision

13. component group orders (or bounds) – this will require implementing quaternion algebra ideal arithmetic.

14. tamagawa numbers

15. analytic rank

16. rational part of special value

17. first 10 zeros in the critical strip

18. leading coefficient of $p$-adic $L$-series for first 10 good primes.
4.2 Factors of $J_0(N)$ for $N \leq 125$

4.3 Factors of $J_H(N)$ for $N \leq 49$

4.4 Minimal Isogenies

Connections with computing curves $X$ whose Jacobian is an $A_f$.

[[Papers of people about this, and they care about whether $A_f$ is isomorphic to its dual. Frey students...]]

4.5 Birch and Swinnerton-Dyer

Connections with BSD. Away from 2 and minimal degree of isogeny, the order of $X$ (mod maximal divisible subgroup) is a perfect square (reference [[william will find]]). Our data is consistent with [[william will find]].

4.6 Other Examples

$J_0(389)$.

[[move this into the paper itself]]

4.7 Level 35

It’s not obvious that $A_f$ is iso. to its dual.

$[35, 2, 2, 1, 6, x^4 + 2x^3 - 7x^2 - 8x + 16]$,

Mention 6-author paper and Hasegawa, but that kernel of modular polarization is NOT kernel of multiplication by an integer, so Wang excludes.

Kernel is $(\mathbb{Z}/2\mathbb{Z})^2$, which is not ker([2]) = $(\mathbb{Z}/2\mathbb{Z})^4$.

> J := JZero(35);
> A := J(2);
> Dual(A);
Modular abelian variety of dimension 2 and level 5*7 over Q
> Kernel(ModularPolarization(A));
Finitely generated subgroup of abelian variety with invariants [ 2, 2 ]

There is a solution, and it gives an iso.

4.8 Level 69: The first $A_f$ that is not isomorphic to $A_f^\vee$

Let $A$ be the second factor in the decomposition of $J_0(69)$. [[Say dim($A$) = 2, etc., which determines $A$.]] Then $A$ is not isomorphic to its dual $A^\vee$ because
there are no solutions to the norm equation [...]. A minimal isogeny between $A$ and $A^{∨}$ is of degree 4 and is given on the integral homology by

$$
\begin{pmatrix}
1 & 0 & 2 & -2 \\
0 & 1 & 0 & 0 \\
-2 & 1 & 0 & 2 \\
4 & -2 & 2 & -4
\end{pmatrix}
$$

[[That’s meaningless without a basis!]]

4.9 Level 195: An $A_f$ not isomorphic to its dual, though there are solutions to the norm equation

\[195, 5, 3, [4, 4, 4, 176, 176], 0, 6, x^6 - 14 \ast x^4 - 4 \ast x^3 + 49 \ast x^2 + 28 \ast x + 4\]

There are solutions to the norm equation, but none of them works.

References


